Online Safety Policy
Beech Hill School

Approved by:	Becky Creighton	**Date:**	July 2023
Last reviewed on:	July 2023		
Next review due by:	July 2024		

Intent

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas, technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The risk of radicalisation
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Aims for pupils

The online safety element of the computing curriculum aims to…

- Protect children from potential dangers online whilst in school
- Educate children in ways of protecting themselves against online dangers on a range of devices they may be exposed to whilst away from school
- Teach children to be considerate and kind when online
- Educate children about the overuse of devices/ games consoles
- Help children to be able to identify fraudulent emails/websites
- Show children how to report online abuse
- Discuss, remind or raise relevant online safeguarding messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Plan any internet use carefully to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.

- Teach children how to use a range of age-appropriate online tools in a safe and effective way.
- When searching the internet for information, pupils will be guided to use age appropriate search engines. All use will be monitored and pupils will be reminded of what to do if they come across unsuitable content.
- Teach children about the impact of cyberbullying and know how to seek help if they are affected by any form of online bullying.
- Make children aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button

Implementation:

This section begins with an outline of the key people responsible for developing our Online Safety Policy and keeping everyone safe with computing. It also outlines the core responsibilities of all users of computing in our school.

It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of computing.

Responsibilities: Online Safety coordinator

Our online safety coordinator is the person responsible to the head teacher and governors for the day to day issues relating to online safety. The online safety coordinator:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident
- Provides training and advice for staff
- Liaises with school computing technical staff
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Reports regularly to Senior Leadership Team
- Receives appropriate training and support to fulfil their role effectively

Responsibilities: Governors

Our governors are responsible for the approval of this policy and for reviewing its effectiveness. This will be carried out by the governors receiving regular information about online safety incidents and monitoring reports. A member of the governing body has taken on the role of online safety governor.

Responsibilities: Head Teacher

- The head teacher is responsible for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety is delegated to the Online safety Co-ordinator
- The head teacher and another member of the senior management team should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. See flow chart on dealing with online safety incidents – below and relevant Local Authority HR / disciplinary procedures)

Responsibilities: classroom-based staff

Teaching and Support Staff are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy and practices
- They have read, understood and signed the school's Acceptable Use Policy for staff
- They report any suspected misuse or problem to the Online safety Co-ordinator
- Digital communications with students and parents via Seesaw should be on a professional level and all messages must be kept as a log of conversation
- Online safety issues are embedded in the curriculum and other school activities.

Responsibilities: Computing Technician

The Computing Technician is responsible for ensuring that:

- The school's computing infrastructure is secure and is not open to misuse or malicious attack
- Users may only access the school's networks through a properly enforced password protection policy
- Shortcomings in the infrastructure are reported to the computing lead or head teacher so that appropriate action may be taken.
- Has responsibility for blocking / unblocking internet sites in the school's filtering system / passing on requests for blocking / unblocking to the Computing Helpdesk
- Maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices

Schedule for development / monitoring / review of this policy

The implementation of this online safety policy will be monitored by:	Online safety coordinator- Becky Creighton
Monitoring will take place at regular intervals:	Annually
The governing body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	July 2023
Should serious online safety incidents take place, the following external persons / agencies should be informed:	Calderdale Safeguarding Children board online safety representative West Yorkshire Police Prevent (if radicalisation is suspected)

The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other online safety incidents covered by this policy, which may take place out of school, but is linked to membership of the school.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate online safety behaviour that take place out of school.

Acceptable use

All members of the school community are responsible for using the school computing systems in accordance with the appropriate acceptable use policy, which they will be expected to sign before being given access to school systems.

Acceptable use policies are provided in Appendix 1 of this policy for:

• Pupils (EYFS + KS1 / KS2)
• Staff (and volunteers)
• Parents / carers (including permissions to use pupil images / work and to use computing systems)
• Community users of the school's Computing system

Acceptable use policies are revisited and resigned annually at the start of each school year and amended accordingly in the light of new developments and discussions with the children which take place at the time. Copies are sent home for further discussion with parents.

For children in EYFS and KS1 parents may sign on behalf of their children

Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy

Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools Computing resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year.

Community users sign when they first request access to the school's computing system. Induction policies for all members of the school community include this guidance.

Planning and Teaching for EYFS- YR 6

Each year group will be taught online safety throughout the year. The units are taken from the scheme from National Online Safety. These units are broken down into 8 units-

- Self-image and identity
- Online relationships
- Online reputation
- Online bullying
- Managing online information
- Health, wellbeing and lifestyle
- Privacy and security
- Copyright and ownership
-

In February of each year, the whole school takes part in Safer Internet Day, where each year group completes activities around a story book.

Children will either be taught in classrooms or the ICT suite, depending on the unit being taught. Their work will either be evidenced on Seesaw, Purple Mash or saved in the shared drive on the school network in the child's own folder. These units of work are age appropriate but can also be adapted to suit the ability of the children.

Monitoring

Computing lead to monitor children's electronic folders to ensure that work has been completed and understood. Children higher up the school will also complete self-assessments. This will help teachers to gauge the understanding of the children.

Other policies relating to online safety

Anti-bullying	How our school strives to eliminate bullying – link to cyber bullying
PSHE- Jigsaw	Online safety has links to this
Safeguarding	Safeguarding children electronically is an important aspect of Online safety. The online safety policy forms a part of the school's safeguarding policy
Behaviour	Linking to positive strategies for encouraging online safety and sanctions for disregarding it.

Illegal or inappropriate activities and related sanctions

The school believes that the activities listed below are inappropriate in a school context (those in **bold and red** are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). Users shall not visit internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- **Child sexual abuse images** (illegal - The Protection of Children Act 1978)
- **Grooming, incitement, arrangement or facilitation of sexual acts against children** (illegal – Sexual Offences Act 2003)
- **Possession of extreme pornographic images** (illegal – Criminal Justice and Immigration Act 2008)
- **Criminally racist material in UK – to stir up religious hatred** (or hatred on the grounds of sexual orientation) (illegal – Public Order Act 1986)
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute

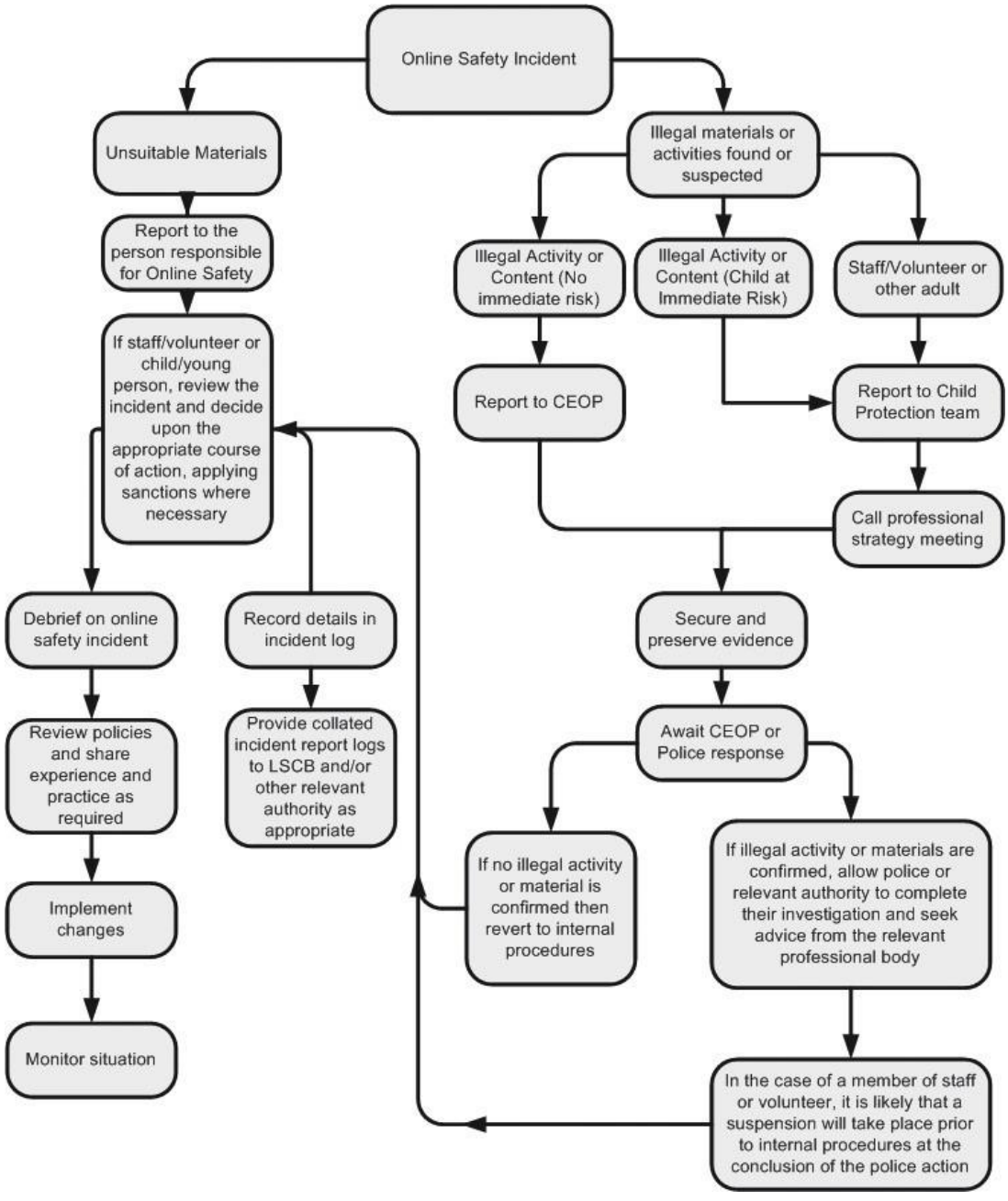
Additionally, the following activities are also considered unacceptable on computing kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.
It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures.

Reporting of online safety breaches

It is hoped that all members of the school community will be responsible users of computing, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:



Audit / Monitoring / Reporting / Review

The Online safety coordinator will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. These records will be reviewed by the head teacher / and a governor on a termly basis.

Use of hand-held technology (personal phones and hand-held devices, tablets or iPads)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

- Personal hand-held devices will be used in lesson time only in an emergency or extreme circumstances- class phones can be used in the majority of situations
- Members of staff are free to use these devices in school, outside teaching time, where children are not present, e.g. staffroom.
- Pupils are not currently permitted to bring their personal hand held devices into school.

Email

Access to email is provided for all staff in school via the intranet page accessible via the web browser (Internet Explorer) from their desktop.

These official school email services may be regarded as safe and secure and are monitored.

- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored
- Pupils have access to a simulated email account through Purple Mash for teaching purposes. This is monitored by teachers
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
- Users must immediately report, to their class teacher / online safety coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- See also the following section for guidance on publication of photographs

- **Use of web-based publication tools**
- Our school uses the public facing website, http://www.beechhillschool.co.uk/site/ for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children. All users are required to consider good practice when publishing content.
- Personal information should not be posted on the school website and only official email addresses
- Parents of all children to fill out a consent form when children start school to consent or refuse use of the child's image, video, name, work etc to be on Seesaw, the school website, the school Twitter account, displays around school, the child's workbooks, the workbooks of other children and the school newsletter. These preferences are to be saved electronically for the child's duration at Beech Hill School. Parents are advised that they can change their preferences at any time by contacting the school office in person, by phone or via email.
- Only pupils' first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
    - Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf . Teachers translate these standards appropriately for all matters relating to online safety.

Any digital communication between staff and pupils or parents / carers (email, Seesaw inbox) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of pupils are used to inform this process also.

Data Protection and GDPR

Personal Data is defined as any data which relate to a living individual who can be identified from the data. This includes opinion about the individual. Sensitive Personal Data about a person includes information about their racial or ethnic origin, political opinions, their religious beliefs or other beliefs of a similar nature, whether they are a member of a trade union and their physical or mental health or condition. Personal data is recorded, processed, transferred and made available according to the General Data Protection Regulation and is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary

- Processed in accordance with the data subject's rights
- Secure and only transferred to others with adequate protection

Transfer of Data

Whenever possible, secure online storage is used to ensure that documents do not need to be transferred to limit the risk. We ensure that data is stored in accordance with the requirements laid down by the Information Commissioner's Office and within the EU. This also applies to cloud storage used. If data has to be transferred via email, it is done with password protection where possible.

Staff training

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff to undertake online safety virtual training via the National College site
- It is expected that some staff will identify online safety as a training need within the performance management process.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school online safety policy and acceptable use policies which are signed as part of their induction
- The Online safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority, the HSCB and others.
- The Online safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Governor training

Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any subcommittee or group involved in computing, online safety, health and safety or child protection. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority (Governor Services or Learning and Achievement Service), National Governors Association or other bodies.
- Participation in school training / information sessions for staff or parents

The online safety governor works closely with the online safety coordinator and reports back to the full governing body

Parent and carer awareness raising

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

• Letters, newsletters, website, Seesaw, Twitter
• Parents' evenings
• Reference to the parents' materials on the Think U Know website (www.thinkuknow.co.uk) or others

Wider school community understanding

The school will offer family learning workshops in computing, media literacy and online safety so that parents and children can together gain a better understanding of these issues. These will take place mostly during parent weeks and will be led by the online safety coordinator. Messages to the public around online safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access school Computing systems / website will be expected to sign a community User AUP before being provided with access to school systems.

APPENDIX 1: Guidelines for Internet and Mobile Telephone Usage

This policy covers all school employees.

Introduction

E-mail, the internet and mobile telephones enable staff to have more ready access to information and colleagues. They transform the way we do our jobs and can enrich the working environment.

They are therefore something to be mentioned and used whenever and wherever possible to streamline communication.

The following "traffic light" system has been produced to help staff make effective use of these technologies:

Red (Do not engage in these activities)

- Use e-mail to engage in gossip
- Make libelous statements about individuals or other organisations
- Make statements purporting to represent the school or the council when they are personal views
- Make derogatory remarks or express derogatory opinions about the school or the council
- Knowingly infringe copyright or intellectual property rights
- Knowingly send or receive anything which is illegal or fraudulent
- Knowingly send or receive material which is obscene, sexually explicit, offensive, defamatory, racist or homophobic in nature, or any material which is intended to cause the receiver or anyone who sees the material harassment, alarm or distress
- Use the facility to pursue personal business interests, for gambling on for political purposes not directly related to your job.
- Allow anyone else to use your user name and password to gain internet access.
- Knowingly engage in any activity, which threatens the integrity or availability of the school's systems.
- Attempt to break into (HACK) any area.
- Allowing mobile phones to ring during working time

Amber (Seek your manager's approval prior to engaging in the activity)

- Opening and/or sending personal e-mails in working time
- Personal purchases of goods and services via the internet in working time
- Use mobile telephones to receive or make / send personal calls or text messages in work time

Green (Legitimate use)

- Communicate by e-mail or mobile phone on behalf of the school or as an aid to pursuing tasks within the employees job remit
- Conducting research into work related matters
- Personal research of the internet or sending personal e-mails outside working hours
- Personal purchases of goods and services via the internet outside working hours
- Opening personal e-mails outside working time
- Receive/sending personal text messages outside working time
- Receiving/making personal calls outside working time

This list is neither exclusive nor exhaustive if you are in any doubt about where you should be using the facility for a particular purpose – consult a member of the Senior Management Team.

Please note that any failure to comply with the policy may constitute gross misconduct and could lead to disciplinary action. If you inadvertently access a site that contains illegal or offensive material, please inform the ICT manager immediately.

APPENDIX 2: Pupil Permissions

Name of Child: _____

Parental Consent and Permission Document

In order to demonstrate your child's achievements and celebrate the life of the school (within the school community and in some instances the wider public), we take photographs and videos as they work and of their work. Under the General Data Protection Regulation (GDPR) we require your consent for using these photographs and videos for the various purposes as set out below.

If you do not give your consent or you do not return the form then we will not use the photographs/videos of your child. If you provide your consent for some of the purposes but not others we will ensure that we follow your wishes.

We ask you as a parent or carer to decide on behalf of your child what can be done with their images.

We would be grateful if you could complete the authorisation document below, and sign and date.

My child can be photographed and filmed for these purposes:	YES	NO
Records of Achievement and record keeping		
School publications and brochures (marketing of the school)		
Website		
Social Media (School's Twitter)		
Seesaw (site used for sharing child's work between school and home)		
Newsletter		
Other media such as local or national press		
Display boards in class and around school		
School trips and Residential		
May we record your child's voice on a computer e.g. during music, on Seesaw?		
May we photograph your child any school productions/performances?		
May we film your child any school productions/performances?		
I give permission for my child to have an individual school photograph taken by a supplier approved by the school.		
I give permission for my child to have a class photograph taken by a supplier approved by the school. I understand this photograph can be purchased by other parents.		
I give permission for my child's first name to used, when appropriate, for the above purposes		

Other Consent:		
Please note that we are required to hold the emergency contact details for your child and we will obviously contact you in the case of an emergency. We also currently use your contact details in order to keep you informed about information relating to the school more generally such as reminders and events. Under the GDPR we require your consent in order to continue to remind you of things via text message in this way.		

I am aware that Beech Hill uses a third party SMS service to contact me by text for school based communication. I agree to the school using this service for non-emergency communication.		
Local Area Walks: I give permission for my child to take part in local outings during school time. This may involve transport, in which case parents will be notified.		
Sports Activities: I give permission for my child to take part in all inter-school sports activities. This will include them being transported to and from the vent (parents will be informed 2 days before the event if their chid is taking part)		
Medical: I give permission for the school to seek medical advice and provide medical treatment in the event of an emergency and/or being unable to contact me.		
Internet Access: (responsible use of the internet): As part of pupils work across the curriculum and the development of pupils' ICT skills, we are providing the children with supervised access to the Internet including e-mail facilities. Our school access provider operates a filtering system that restricts access with inappropriate materials. Whilst every endeavour is made to ensure that suitable restrictions are in place to reduce the chances of children accessing inappropriate materials, the school cannot be help responsible for the nature or content of materials accessed through the Internet. The school will not be liable for any damages arising from your child's use of the Internet facilities.		

Signed (parent/ guardian: _____ Date: _____

Updated November 2022

I understand that the consent provided is for the duration of my child's time at the school.

I understand that I can withdraw consent by completing and returning a Consent Withdrawal or Alteration form which is available from the school office and published on the website.

This will be acted on within 5 working days of term time:

Child's name (PRINT) ……..……..……..

Parents/Carers Name
(PRINT)……..……..……..

Signature of parent/carer(s)
……..…….……Date……
….

Updated November 2022